

Remarks

*Claim Rejections - 35 USC § 102 (e)*

The Examiner has rejected claims 1-32 as being anticipated by Tetro et al. (U.S. Pat. No. 6,122,624). Examiner states that,

“as per claims 1, 14-16, 24-27, and 31 Tetro discloses a method/system for enhanced fraud detection in electronic purchase transactions from a remote site (which is readable as Applicant’s claimed invention wherein it is stated that a method for detecting fraud non-personal transactions), comprising the steps of:

transmitting the purchaser’s data to a fraud-detection system, the purchaser’s data including a ship-to-address for the transaction (see., abstract, specifically wherein it is stated that an electronic purchase is prompted to input the user’s billing address and social security number, col 5, lines 47-59, the enhanced fraud detection system 10);

processing the purchaser’s data to determine whether the transaction is potentially fraudulent (see., abstract, specifically wherein it is stated that a determination is made whether the account associated with the social security number has been authorized for use, col 2, lines 39-61, please note that the process for matching the user’s billing address and social security number is equivalent to the step of determining for potential fraud);

returning the relative risk of fraudulent activity associated with the transaction (see., abstract, col 2, lines 49-67, specifically wherein it is stated that if the social security number falls into any of these categories, then authorization for the purchase is refused).”

Applicants respectfully disagree with the Examiner’s assertion that Tetro et al. disclose a method/system comprising the steps of “transmitting the purchaser’s data to a fraud-detection system, the purchaser’s data including a ship-to-address for the transaction”. The Examiner has noted correctly the teachings of Tetro et al. in the following sentence from the Office Action: “(see, abstract, specifically wherein it is stated that an electronic purchase is prompted to input the user’s billing address and social security number, col 5, lines 47-59, the enhanced fraud

detection system 10)". As can be appreciated, the "ship-to-address" may be different from the "user's billing address". An important distinction between the ship-to-address and the user's billing address is highlighted in the Applicants' "Background of the Invention" beginning on page 2, line 22 through page 3, line 4 which states,

The electronic merchant receives an order from the person who gives a name, credit card number, and expiration date to the retailer in connection with a purchase. The purchaser directs that the merchandise be delivered to an address which is different than the credit card billing address. Using traditional methods, the merchant receives a credit card approval number from its gateway and ships the merchandise to the shipping address.

If, in fact, the credit card number has been stolen and the transaction is fraudulent, the true cardholder will likely reject the invoice when he is billed for it, claiming fraud. Since the credit card company had confirmed the validity of the card (which remains in the owner's possession), and because the transaction is "card not present", i.e., was not involved with a signature verification, the credit card company has no liability. Assuming the cardholder refuses to pay the credit card company, the credit company will issue a charge back against the retailer, which has no recourse."

Transmitting the "ship-to address for the transaction", as is claimed in Applicant's novel method that includes claim 1, permits "checking the purchaser's ship-to address against a historical database to determine whether a pattern of fraudulent activity exists for the ship-to address; and checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends". (page 3, lines 21-26).

Checking the ship-to address provides benefits not available with other methods.

For example, if a merchant database reveals that there have been one or more deliveries to a specified ["ship-to"] address without objection by the cardholder, it is almost certain that further deliveries to that address (particularly if

it matches the cardholder's address) are legitimate. If, however, a delivery is directed to an address inconsistent with the existing pattern associated with that critical purchase, it will trigger an alert that the transaction may be fraudulent. In such an event, the merchant will telephone or use the "safe-call" call verification program to communicate with the card owner to get confirmation of the bona fides of the transaction. (page 6, lines 13-27).

*Claim Objections*

The Examiner has objected to Claim 1 because of a informality. The Examiner has advised Applicant to remove the word "is" and replace it by --in--.

Applicant has amended the claim in accordance with the Examiner's suggestion.

Considering the foregoing, it is sincerely believed that this case is in a condition for allowance, which is respectfully requested.

\* \* \* \* \*

This paper is intended to constitute a complete response to the outstanding Office Action. Please contact the undersigned if it appears that a portion of this response is missing or if there remain any additional matters to resolve. If the Examiner feels that processing of the application can be expedited in any respect by a personal conference, please consider this an invitation to contact the undersigned by phone.

**Please note new Power of Attorney forms attached. Please direct all future correspondence to Customer Number 22206.**


Respectfully submitted,

11/21/03  
DATE

Reg. No.: 36,050

Tel. No.: (918) 599-0621

Customer No.: 22206

  
SIGNATURE OF PRACTITIONER

R. Alan Weeks  
(type or print name of practitioner)

321 S. Boston Ave., Suite 800  
P.O. Address

Tulsa, OK 74103-3318